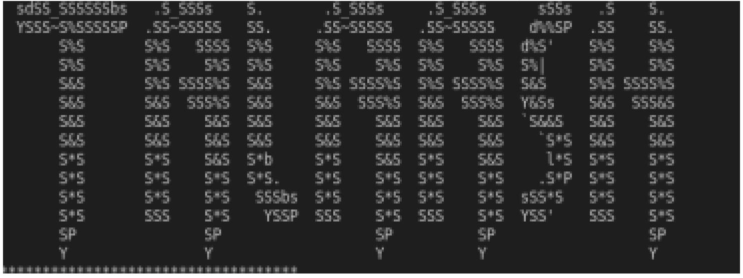
A
Project Report
On
"Website Penetration Testing Tool"

(CE351 – Software Group Project III)



Prepared by

Akshat Shah (17CE102)
Keyur Talati (17CE124)

Under the Supervision of

Dr. Parth Shah
Prof. Pritesh Prajapati
Prof. Sneha Padhiar
Prof. Dipsi Dave

Submitted to

Charotar University of Science & Technology (CHARUSAT)
for the Partial Fulfillment of the Requirements for the
Degree of Bachelor of Technology (B.Tech.)
in Computer Engineering (CE)
for 6th semester B.Tech.

Submitted at

CHARUSAT
CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

Accredited with Grade A by NAAC
Accredited with Grade A by KCG

cspit
Chandubhai S Patel Institute of Technology

U & P U. PATEL DEPARTMENT OF COMPUTER ENGINEERING
(NBA Accredited)
Chandubhai S. Patel Institute of Technology (CSPIT)
Faculty of Technology & Engineering (FTE), CHARUSAT
At: Changa, Dist: Anand, Pin: 388421.
April, 2020

DECLARATION BY THE CANDIDATES

We hereby declare that the project report entitled “**Website Penetration Testing Tool**” submitted by us to Chandubhai S. Patel Institute of Technology, Changa in partial fulfilment of the requirement for the award of the degree of **B.Tech.** in Computer Engineering, from U & P U. Patel Department of Computer Engineering, CSPIT/FTE, is a record of bonafide CE351 Software Group Project III (project work) carried out by us under the guidance of **Prof. Sneha Padhiar, Prof. Kruti Dhyani, Prof. Dipsi Dave** . We further declare that the work carried out and documented in this project report has not been submitted anywhere else either in part or in full and it is the original work, for the award of any other degree or diploma in this institute or any other institute or university.

Akshat Shah (17CE102)
Keyur Talati (17CE124)

Dr. Parth Shah
H.O.D I.T.
Smt. Kundanben Dinsha Patel Department of Information Technology,
CSPIT/FTE, CHARUSAT-Changa.

Prof. Pritesh Prajapati
Asst. Professor
Smt. Kundanben Dinsha Patel Department of Information Technology
CSPIT/FTE, CHARUSAT-Changa.

Prof. Sneha Padhiar
Asst. Professor
U & P U. Patel Department of Computer Engineering,
CSPIT/FTE, CHARUSAT-Changa.

Prof. Kruti Dhyani
Asst. Professor
U & P U. Patel Department of Computer Engineering,
CSPIT/FTE, CHARUSAT-Changa.

Prof. Dipsi Dave
Asst. Professor
U & P U. Patel Department of Computer Engineering,
CSPIT/FTE, CHARUSAT-Changa

CHARUSAT
CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

Accredited with Grade A by NAAC
Accredited with Grade A by KCG

CERTIFICATE

This is to certify that the report entitled "**Website Penetration Testing Tool**" is a bonafied work carried out by **Akshat Shah (17CE102)** under the guidance and supervision of **Prof. Sneha Padhiar, Prof. Kruti Dhyani,Prof. Dipsi Dave** for the subject **Software Group Project III (CE351)** of 6th Semester of Bachelor of Technology in **Computer Engineering** at Chandubhai S. Patel Institute of Technology (CSPIT), Faculty of Technology & Engineering (FTE) – CHARUSAT, Gujarat.

To the best of my knowledge and belief, this work embodies the work of candidate herself, has duly been completed, and fulfills the requirement of the ordinance relating to the B.Tech. Degree of the University and is up to the standard in respect of content, presentation and language for being referred by the examiner(s).

Under the supervision of,
Prof. Sneha Padhiar
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Prof. Kruti Dhyani
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Prof. Dipsi Dave
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Dr. Ritesh Patel
Head - U & P U. Patel Department of Computer Engineering,
CHARUSAT, Changa, Gujarat.

Chandubhai S. Patel Institute of Technology (CSPIT)

Faculty of Technology & Engineering (FTE), CHARUSAT

At: Changa, Ta. Petlad, Dist. Anand, Pin:388421. Gujarat.

CHARUSAT
CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

Accredited with Grade A by NAAC
Accredited with Grade A by KCG

CERTIFICATE

This is to certify that the report entitled "**Website Penetration Testing Tool**" is a bonafied work carried out by **Akshat Shah (17CE102)** under the guidance and supervision of **Prof. Sneha Padhiar, Prof. Kruti Dhyani,Prof. Dipsi Dave** for the subject **Software Group Project III (CE351)** of 6th Semester of Bachelor of Technology in **Computer Engineering** at Chandubhai S. Patel Institute of Technology (CSPIT), Faculty of Technology & Engineering (FTE) – CHARUSAT, Gujarat.

To the best of my knowledge and belief, this work embodies the work of candidate herself, has duly been completed, and fulfills the requirement of the ordinance relating to the B.Tech. Degree of the University and is up to the standard in respect of content, presentation and language for being referred by the examiner(s).

Under the supervision of,
Prof. Sneha Padhiar
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Prof. Kruti Dhyani
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Prof. Dipsi Dave
U & P U. Patel Dept. of Computer Engineering.
CSPIT/FTE, CHARUSAT, Changa, Gujarat

Dr. Ritesh Patel
Head - U & P U. Patel Department of Computer Engineering,
CHARUSAT, Changa, Gujarat.

Chandubhai S. Patel Institute of Technology (CSPIT)

Faculty of Technology & Engineering (FTE), CHARUSAT

At: Changa, Ta. Petlad, Dist. Anand, Pin:388421. Gujarat.

Abstract

The world is very reliant on the Internet. Nowadays, web security is the biggest challenge in the corporate world. Web application are prone to security attacks. Web security means to secure the web application layer from the attacks by unauthorized attackers/users. Many issues that occur on web is mainly due to improper inputs by the client. The main elements of web security techniques such as the passwords, encryption, authentication and integrity.

Acknowledgement

We deem it as a privilege to thank Dr. A.D. Patel, Principal, CSPIT, CHARUSAT and Dr. Ritesh Patel, HOD, CSPIT, CHARUSAT for fostering an excellent academic environment in this institution, which made this endeavour fruitful. We would like to express our sincere gratitude to Prof. Sneha Padhiar, Prof. Kruti Dhyani,Prof. Dipsi Dave SGP Faculty, for her incredible guidance and encouragement and valuable suggestions that enabled us to complete this project successfully. We thank non-teaching staff members of Department of Computer Engineering, CSPIT for their support during this project work. Above all, we would like to thank our parents for their unconditional support all along.

Table of Contents

List of Figures

Chapter 1: Introduction

Web security is an important aspect of web applications. Today web security is very concerned related to Internet. Most modern website and Web applications are employed to carry out most major tasks, which can collect the personal, secret and private information such as health history, debit, credit card information and many more. The security of a computer system is important to other protection to the system and the data store in it.

Web applications are a main base of attacks such as cross-site scripting, cookie-session theft, browser attack, self-propagating worms in web email and web sites. These types of attacks are called 'injection attacks' which attacks by the use of malicious code. Injection attacks have commanded the highest purpose of web application vulnerability lists for a major a part of the previous decade.

What is Vulnerability?

In Computer Security: "A Vulnerable is a weakness which allows an attacker to reduce a system's information assurance".

Vulnerability is a cyber-security term that refers to the flaw in a system or web application that can leave it to open to an attack. A vulnerability may also refer to any type of weakness into any system/ web applications anything that leaves information security exposed to a threat.

What is Exploit?

"An Exploit means to take advantage of something for one's own end, especially unethically."

Exploitation is the next step in an attacker's playbook after finding a vulnerability. Exploits are the means through which a vulnerability can be used for malicious activity by hackers; these include pieces of software, sequences of commands, or even open-source exploit kits.

What is Threat?

A Threat is an event when an attacker uses the vulnerability. The threat itself will normally have an exploit involved. As it is the common way where hackers make their move. A hacker may use multiple exploits and demand for some type of rewards in return. Well now its upon attacker whether he want to misuse this exploits or wants to inform these exploits to the client.

Chapter 2: Top 10 Web Attacks

In 2020, “OWASP TOP 10” have listed the top current Vulnerabilities which are most critical risk.

2.1 Top 10 Vulnerabilities

1. Sensitive Data Exposure.
2. XML External Entities (XEE)
3. Broken Access Control.
4. Security Misconfiguration.
5. Cross-Site Scripting.
6. Insecure Deserialization.
7. Using Components with Known Vulnerabilities.
8. Insufficient Logging and Monitoring. Common Threats. Man-In-The-Middle Attack. Brute Force Attack.

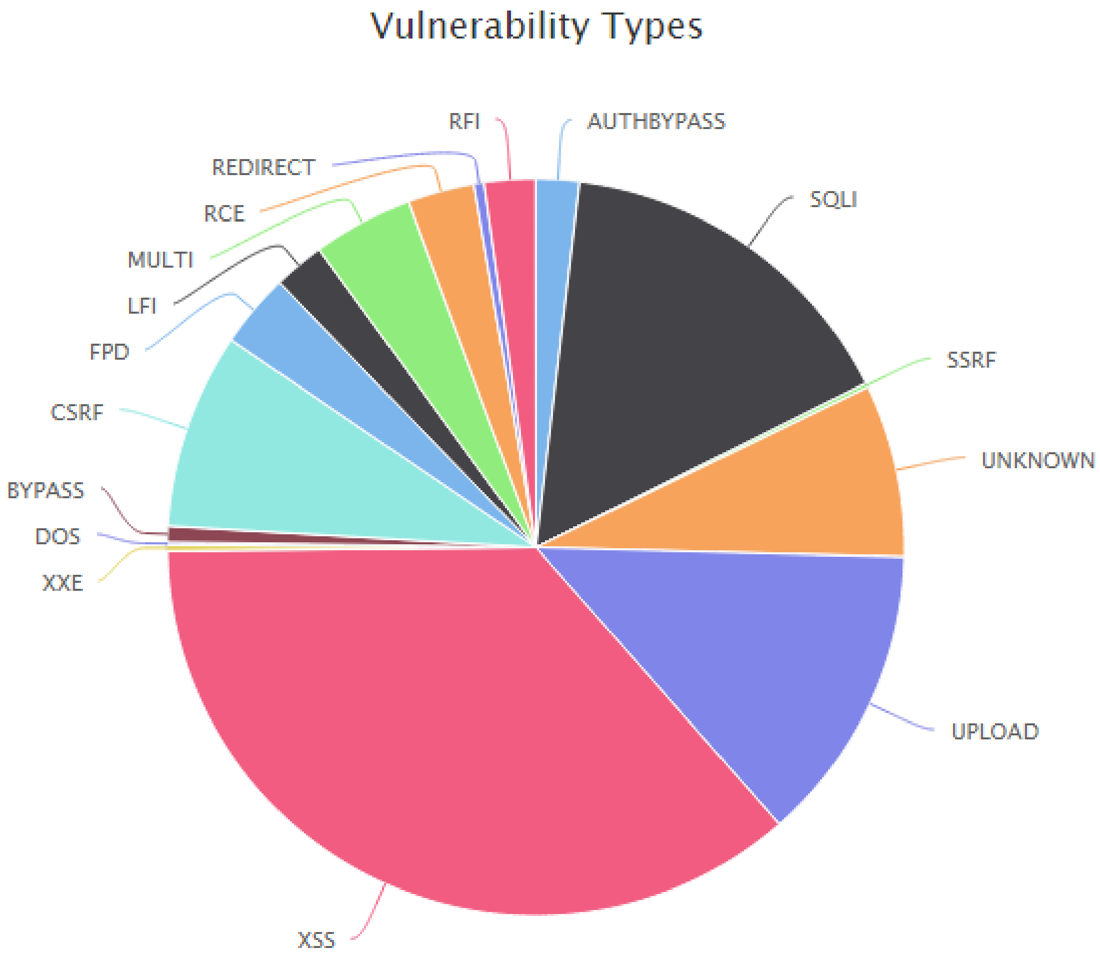


Figure 2.1: Types of Vulnerabilities

2.1.1 Injection

The Injection attack refer to a broad class of attack vectors that allow an attacker to inject any malicious input to a program in the form of script, which gets processed by the interpreter as a part of a command or query which alters the course of execution of the program. Injection is the major problem in Web applications.

The Types of Injections, which are possible are:

SQL Injection (SQLi)

SQL injection is one of the major web security vulnerability that allows an attacker to inject SQL commands that can read, modify data from the database. Advanced variation of the SQL can be used to write arbitrary files to the server and executes OS commands.

2.1.2 Broken Authentication

Vulnerabilities in authentication systems can give attackers access to admin accounts and even gets permission to compromise the entire system using the admin account. Some strategies to mitigate authentication vulnerabilities are requiring 2-factor authentication

2.1.3 Sensitive Data Exposure

Sensitive data exposure takes place when an application, organization, or other substance accidentally uncovered individual information. Its information introduction varies from an information break, in which an assailant gets too and takes data. Sensitive data exposure happens because of not satisfactorily ensuring a database where data is put away. This may be an aftereffect of a huge number of things, for example, frail encryption, no encryption, programming imperfections, or when somebody erroneously transfers information to a wrong database.

2.1.4 XML External Entity Attack

XXE is External Entity attack and is now increasingly found and reported in majority of web applications including Facebook, PayPal etc. It is type of attack against any application that uses XML input. This attack generally occurs when a weakly configured XML parser processes any XML input, which is containing a reference to an external entity. This attack may lead to deleterious impacts of disclosure of confidential data, denial of service, server side request forgery and other system impacts. Various different type of entities such as external general parsed entity often shortened as external entity is used to access remote or local content by declared system identifier.

2.1.5 Broken Access Control

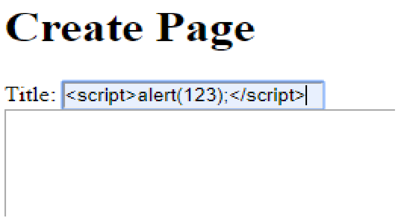
Access control, sometimes called authorization, is how a web app provides access to content and functions to some users and others. These checks are performed after authentication and control what users 'authorized' users can do. Access control seems like a common problem, but difficult to implement properly. The access control model of a web application is closely related to the content and function that the site provides. Additionally, users fall into multiple groups or roles with different capabilities or privileges.

2.1.6 Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show user overly descriptive errors, which may reveal vulnerabilities in the application. This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.

2.1.7 Cross-Site Scripting

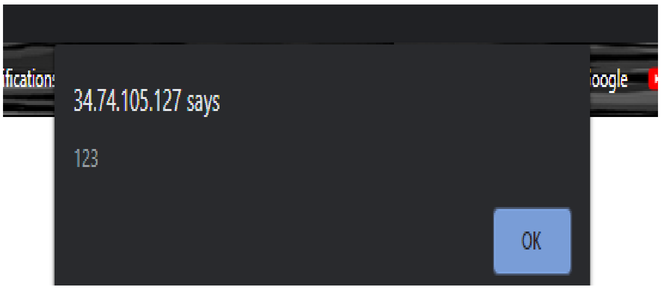
Cross Site Scripting is the most common attack, in which malicious scripts are injected into the websites. XSS attacks occurs generally in the form of browser side script, to an end user. An attacker can use XSS to send a malicious script to an unsuspecting user. The end users browser has no way to know that the script should not be trusted.



Create Page

Title: <script>alert(123);</script>

Figure 2.2: How payload is set



34.74.105.127 says

123

Figure 2.3: Exploited

2.1.8 Insecure Deserialization

This threat targets the many web applications, which frequently serialize and deserialize data. Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it. Deserialization is just the opposite: converting serialized data back into objects the application can use. Serialization is sort of like packing furniture away into boxes before a move, and deserialization is like unpacking the boxes and assembling the furniture after the move. An insecure deserialization attack is like having the movers tamper with the contents of the boxes before they are unpacked.

2.1.9 Using Components with known Vulnerabilities

Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks. Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.

2.1.10 Insufficient Logging and Monitoring

This assumes a real and responsible approach that web applications will be attacked. The main parts of are mentioned below:

1. Logging: Recording one thing that happened is known as logging. Few folks write diaries to record their daily existence in a book. In addition, for any application or website a log contains logins and transactions. These logs are vital and tells us about system failures like access control failure and input validation failures. These types of entries can be useful for detecting malicious activity and solving ahead of it before it has a chance to cause any harm.

2. Monitoring: Collecting records is good, but if no one is looking at those record at times of difficulty then there is no use of it. Monitoring is looking in records for errors or anomalies in records to indicate any failure.

Chapter 3: Vulnerabilities at glance

The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. One of OWASP's core principles is that all of their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security. The materials they offer include documentation, tools, videos, and forums. Perhaps their best-known project is the OWASP Top 10.

The OWASP Top 10 is a regularly updated report outlining security concerns for web application security, focusing on the 10 most critical risks. A team of security experts from all over the world puts the report together. OWASP refers to the Top 10 as an 'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.

3.1 About Owasp top 10

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML external entity
5. Broken access control
6. Security Misconfiguration
7. Cress-Site Scripting
8. Insecure Deserialization
9. Using component with known vulnerability
10. insufficient login and monitoring

Different company have different levels of website vulnerability like burpsuite have major three levels of vulnerabilities where as Owasp has 4 level of vulnerabilities
Here we are talking about three types of vulnerability as per our tool
1) Easy or informatics
2) Medium
3) Hard or Critical

3.1.1 Easy or Informatics

This types of vulrabiloed are connected with the infromantion part of a website like the open ports , DNS record , Whois lookup etc.
Some of the examples are

- Password submission using get method
- url injection
- file upload functionality
- open port list

3.1.2 Medium

Medium levels of vulnerabliti can give you some of the information you want like the cookie detail , backend detail , the cipher detail etc
Some of the examples are

- XML injection

- Cross-Site request forgery
- SMTP header injection
- Password value set in cookie etc

3.1.3. Hard or Critical

This types of vulnerability can damage the whole database and website too. If a hacker find any one of the following vulnerability in the website than it will be a golden mine for him

- SQL injection
- OS command injection
- PHP code injection
- Cross site scripting etc

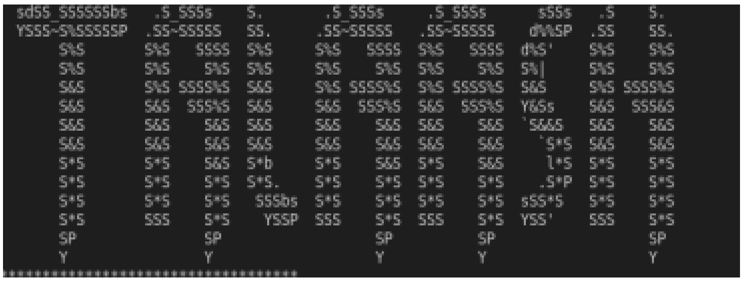
3.2 About CVSS

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

CVSS V3 SCORE	TYPE
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

Chapter 4: TALAASH



```
sdSS_SSSSSSbs   .S_SSSs    S.       .S_SSSs     .S_SSSs      sSSs   .S    S.
YSSS~S%SSSSSP  .SS~SSSSS   SS.     .SS~SSSSS   .SS~SSSSS    d%%SP  .SS    SS.
     S%S       S%S   SSSS  S%S     S%S   SSSS  S%S   SSSS  d%S'    S%S    S%S
     S%S       S%S    S%S  S%S     S%S    S%S  S%S    S%S  S%|     S%S    S%S
     S&S       S%S SSSS%S  S&S     S%S SSSS%S  S%S SSSS%S  S&S     S%S SSSS%S
     S&S       S&S  SSS%S  S&S     S&S  SSS%S  S&S  SSS%S  Y&Ss    S&S  SSS&S
     S&S       S&S    S&S  S&S     S&S    S&S  S&S    S&S  `S&&S   S&S    S&S
     S&S       S&S    S&S  S&S     S&S    S&S  S&S    S&S    `S*S  S&S    S&S
     S*S       S*S    S&S  S*b     S*S    S&S  S*S    S&S     l*S  S*S    S*S
     S*S       S*S    S*S  S*S.    S*S    S*S  S*S    S*S    .S*P  S*S    S*S
     S*S       S*S    S*S   SSSbs  S*S    S*S  S*S    S*S  sSS*S   S*S    S*S
     S*S       SSS    S*S    YSSP  SSS    S*S  SSS    S*S  YSS'    SSS    S*S
     SP                SP                  SP          SP                  SP
     Y                 Y                   Y           Y                   Y
**********************************
```

Figure : TALAASH Logo

TALAASH means Spoofing. Spoofing is very much important for Penetration Testing. Spoofing means when attacker impersonates another user or device on a network, and manipulate the user into believing that they are communicating or interacting with a different person or website.

TALAASH tool is based on java and the tool runs only on **KALI Linux OS**, as it KALI OS is completely security based OS so it is easy for anyone to perform security activities.

As the tool is divided into 3 section,

1. Easy
2. Medium
3. Expert

4.1 Easy

Easy Level auditing is performed by those who are new to Security, who has no knowledge in security or in technical field. Easy option are for those who just want some basic information about the website like,

- **Basic Details:** A whois Kali linux command is a utility as a part of the information gathering used in all of the Linux-based operating systems. this tool is part of information security assessment, and one of information gathering techniques

- **Name Server:** nslookup command. nslookup (name server lookup) is a tool used to perform DNS lookups in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain.

- **Port Scan:** Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

- **Emails and Subdomains of the websites:** This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.

- **File Search:** Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS

- **Domain Name Server:** WAFW00F is a Python tool to help you fingerprint and identify Web Application Firewall (WAF) products. It is an active reconnaissance tool as it actually connects to the web server, but it starts out with a normal HTTP response and escalates as necessary.

4.2 Medium

Medium Level are for those who has knowledge in technical field, who has information how the website works, what are open ports, Headers of the websites and many more. So As an attacker or a Pentester the first step is to gather information about particular website. The tools include in this option are,

- **Port Scan:** nmap --top-ports option by default launches a TCP scan, and figuring out how to do both a TCP and a UDP scan at the same time isn't intuitive for everyone. All you do is precede your scan with the -s option, combined with the type of scans you want to do.

- **Finding DNS Records:** dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

- **SSL Cipher Suites:** SSLScan is a fast SSL port scanner. It connects to SSL ports and determines what ciphers are supported, which are the servers preferred ciphers, which SSL protocols are supported and returns the SSL certificate. Client certificates / private key can be configured and output is to text / XML.

- **Analyze SSL Configuration :** SSLyze is a Python tool that can analyze the SSL configuration of a server by connecting to it. It is designed to be fast and comprehensive, and should help organizations and testers identify mis-configurations affecting their SSL servers.

4.3 Expert

Expert Level are for those who are a security person, who works for securing the websites. This option helps performing attacks to the website to find the vulnerabilities.

This type of Auditing is performed related attacks that helps them to secure their own targets. Types of tools included are

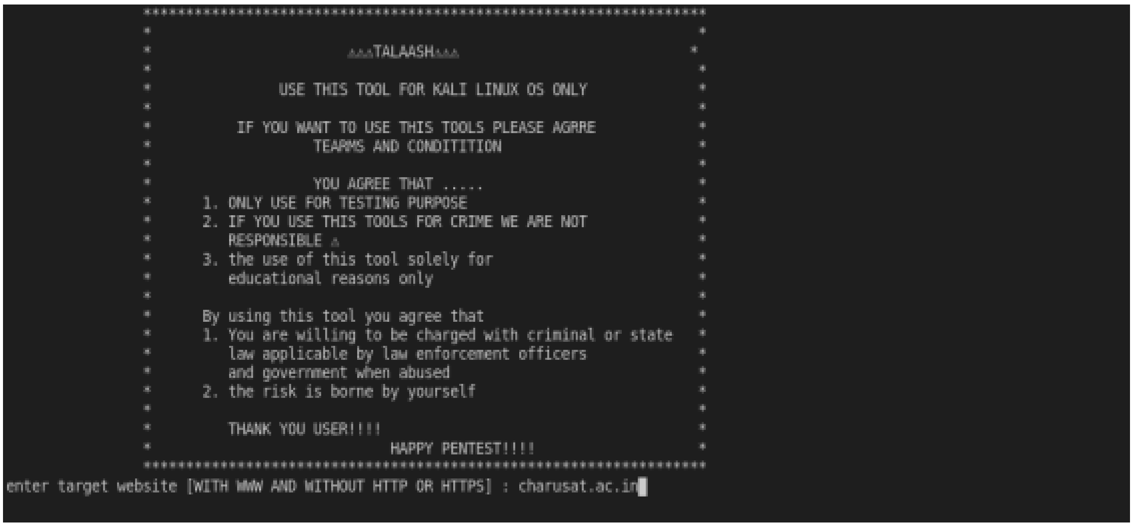
- **Name Server (Expert):-** Nameserver lookup or NS Lookup is a tool for getting name server records of any domain name. NS is a record type of DNS, and it is set up via a hosting provider. Whenever a browser sends a DNS request to DNS server, it sends back the nameserver records, and the name servers are then used to get real IP address behind a domain name. So, it's handy to verify your Nameserver records to check if they are correctly entered in your hosting management interface to avoid any downtime.
- **Port Scan:-** Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what

devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

- **SSL Vulnerability** A2SV is an open source tool used for scanning SSL vulnerabilities in web applications. A2SV performs vulnerability scanning for CCS injection, Heartbleed, Logjam, Freak Attack, Anonymous Cipher, SSL v3 POODLE, SSL v2 Drown, and Crime (SPDY). CCS is the OpenSSL vulnerability that acts as Man in the Middle (MITM) to intercept network traffic and eavesdrop on communications through access to the SSL handshake.
- **Open Ports Vulnerabilities**:- On modern operating systems, ports are numbered addresses for network traffic. Different kinds of services use different ports by default.
- **Wordpress Scan**:- WPScan is a black box vulnerability scanner for WordPress websites. WPScan comes pre-installed in Kali Linux. Kali Linux is a popular Linux distribution built on Debian Kali Linux that comes with many of the best ethical hacking tools pre-installed
- **XSS,CSRF Attack Scan:-** Wapiti is an open source tool that scans web applications for multiple vulnerabilities including data base injections, file disclosures, cross site scripting, command execution attacks, XXE injection, and CRLF injection. The database injection includes SQL, XPath, PHP, ASP, and JSP injections. Command execution attacks include eval(), system(), and passtru() vulnerabilities.

Chapter 5: How TALAASH works

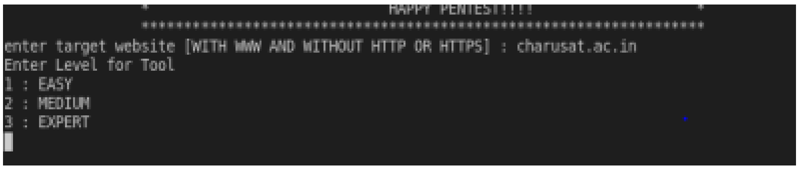
1. First, as you run the tool, you have to enter the website to which you want to test.



```
                  ********************************************************************
                  *                                                                  *
                  *                          ⚠⚠⚠TALAASH⚠⚠⚠                         *
                  *                                                                  *
                  *                  USE THIS TOOL FOR KALI LINUX OS ONLY            *
                  *                                                                  *
                  *             IF YOU WANT TO USE THIS TOOLS PLEASE AGRRE           *
                  *                      TEARMS AND CONDITITION                      *
                  *                                                                  *
                  *                      YOU AGREE THAT .....                        *
                  *          1. ONLY USE FOR TESTING PURPOSE                         *
                  *          2. IF YOU USE THIS TOOLS FOR CRIME WE ARE NOT           *
                  *             RESPONSIBLE ⚠                                        *
                  *          3. the use of this tool solely for                      *
                  *             educational reasons only                             *
                  *                                                                  *
                  *          By using this tool you agree that                       *
                  *          1. You are willing to be charged with criminal or state *
                  *             law applicable by law enforcement officers           *
                  *             and government when abused                           *
                  *          2. the risk is borne by yourself                        *
                  *                                                                  *
                  *             THANK YOU USER!!!!                                   *
                  *                                HAPPY PENTEST!!!!                 *
                  ********************************************************************
enter target website [WITH WWW AND WITHOUT HTTP OR HTTPS] : charusat.ac.in
```

Figure 5.1: Asks user to enter website

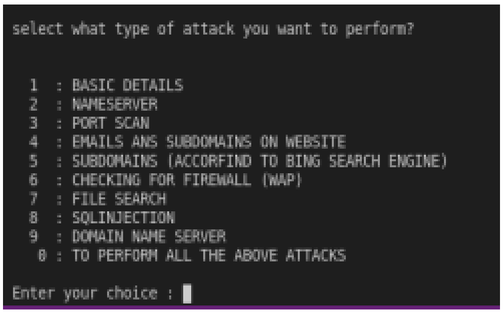
2. After entering website’s URL you have to select the option i.e Easy, Medium, Expert



```
                  *                                HAPPY PENTEST!!!!                 *
                  ********************************************************************
enter target website [WITH WWW AND WITHOUT HTTP OR HTTPS] : charusat.ac.in
Enter Level for Tool
1 : EASY
2 : MEDIUM
3 : EXPERT
```

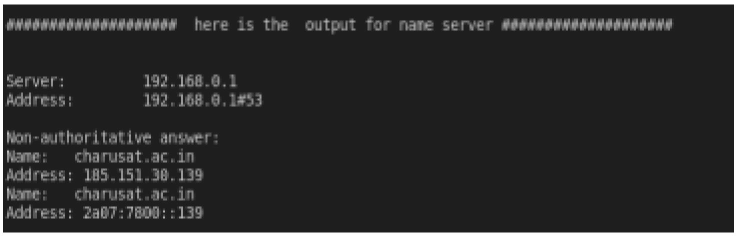
Figure 5.2: User Selects Options

3. If (option = 1) Easy



```
select what type of attack you want to perform?


  1  : BASIC DETAILS
  2  : NAMESERVER
  3  : PORT SCAN
  4  : EMAILS ANS SUBDOMAINS ON WEBSITE
  5  : SUBDOMAINS (ACCORFIND TO BING SEARCH ENGINE)
  6  : CHECKING FOR FIREWALL (WAP)
  7  : FILE SEARCH
  8  : SQLINJECTION
  9  : DOMAIN NAME SERVER
   0 : TO PERFORM ALL THE ABOVE ATTACKS

Enter your choice :
```

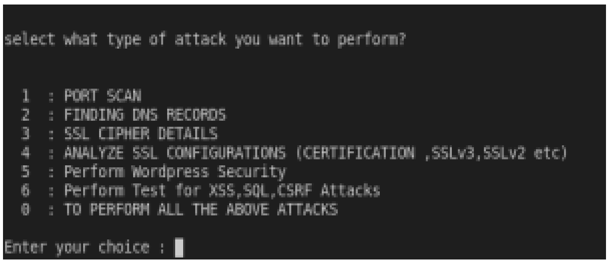
Figure 5.3: Easy Option



```
####################  here is the  output for name server ####################


Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   charusat.ac.in
Address: 185.151.30.139
Name:   charusat.ac.in
Address: 2a07:7800::139
```

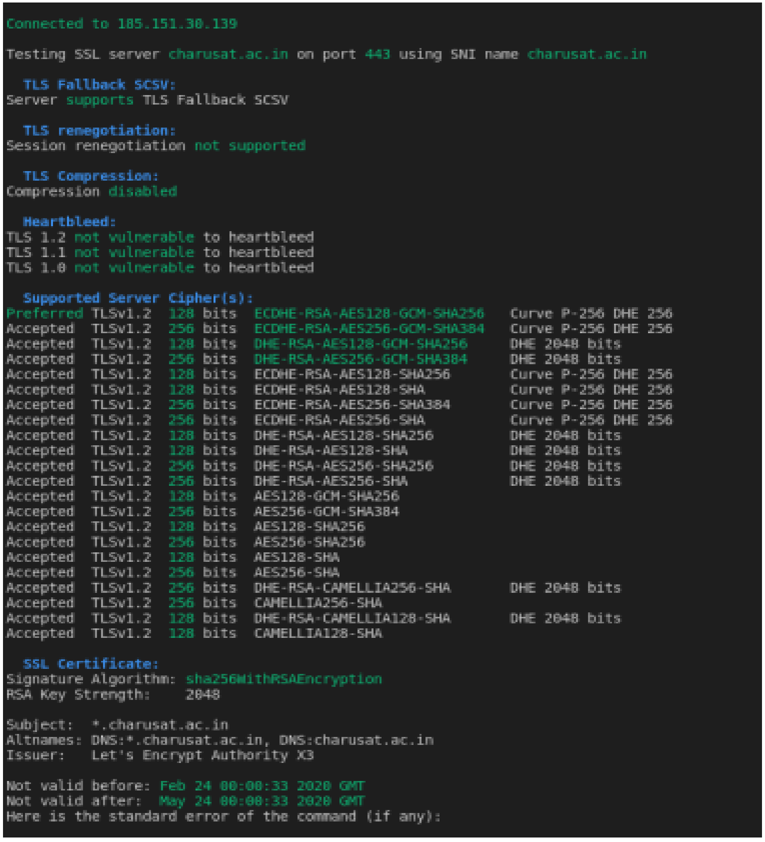
Figure 5.4: Name Server for Easy

4. If (option = 2) Medium



```
select what type of attack you want to perform?


  1  : PORT SCAN
  2  : FINDING DNS RECORDS
  3  : SSL CIPHER DETAILS
  4  : ANALYZE SSL CONFIGURATIONS (CERTIFICATION ,SSLv3,SSLv2 etc)
  5  : Perform Wordpress Security
  6  : Perform Test for XSS,SQL,CSRF Attacks
  0  : TO PERFORM ALL THE ABOVE ATTACKS

Enter your choice : █
```

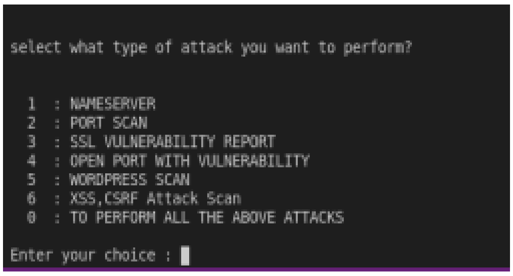
Figure 5.5: Medium Option



```
Connected to 185.151.30.139

Testing SSL server charusat.ac.in on port 443 using SNI name charusat.ac.in

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 2048 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA       DHE 2048 bits
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.charusat.ac.in
Altnames: DNS:*.charusat.ac.in, DNS:charusat.ac.in
Issuer:   Let's Encrypt Authority X3

Not valid before: Feb 24 00:00:33 2020 GMT
Not valid after:  May 24 00:00:33 2020 GMT
Here is the standard error of the command (if any):
```

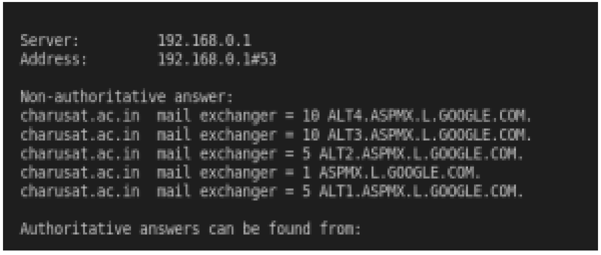
Figure 5.6: SSL Details (Medium)

5. If (option = 3) Expert



```
select what type of attack you want to perform?


  1  : NAMESERVER
  2  : PORT SCAN
  3  : SSL VULNERABILITY REPORT
  4  : OPEN PORT WITH VULNERABILITY
  5  : WORDPRESS SCAN
  6  : XSS,CSRF Attack Scan
  0  : TO PERFORM ALL THE ABOVE ATTACKS

Enter your choice : █
```

Figure 5.7: Expert Option



```
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
charusat.ac.in  mail exchanger = 10 ALT4.ASPMX.L.GOOGLE.COM.
charusat.ac.in  mail exchanger = 10 ALT3.ASPMX.L.GOOGLE.COM.
charusat.ac.in  mail exchanger = 5 ALT2.ASPMX.L.GOOGLE.COM.
charusat.ac.in  mail exchanger = 1 ASPMX.L.GOOGLE.COM.
charusat.ac.in  mail exchanger = 5 ALT1.ASPMX.L.GOOGLE.COM.

Authoritative answers can be found from:
```

Figure 5.8: Name Server (Expert)

Chapter 6: Conclusion & Future Enhancement

Conclusion

The reasons are fairly clear as to why penetration testing should be performed on a regular basis. The need for the kind of offensive approach to security breach defence is especially important in systems that have valuable or sensitive information stored, such as customer data bases, financial records, medical records, a company’s sales reports, legal documentation, etc.

Penetration tests attempt to emulate a 'real world' attack to a certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. If the penetration tester finds 5 holes in a system to get in this does not mean that hackers or external intruder will not be able to find 6 holes.

Future Enhancement

- As this tool is completely based on Kali Linux OS we will try to convert this tool to multiple OS
- We will try to generate a report in the form of PDF
- We will try to make this tool a WEB based tool and also to secure the tool
- We will also try to add more tools so that this tool performs more testing.

Chapter 7: Bibliography

- https://owasp.org/www-project-top-ten/
- https://www.whitehatsec.com/faq/content/top-vulnerabilities-list
- https://lp.skyboxsecurity.com/rs/skyboxsecurity/images/Skybox_Report_Vulnerability_Threat_Trends_18.pdf
- https://tools.kali.org/tools-listing
- https://linuxhint.com/top-25-best-kali-linux-tools/